In the Specification:

Please replace the paragraph beginning at page 7, line 5, and ending at page 7, line 8, with the following rewritten paragraph:

-- ~~Alernatively~~Alternatively, the authenticatable device may send the initial message to the communicator authorizing said activity, before or after the non-authenticatable device attempts to access the service. The reply may then contain an identifier to be used by the non-authenticatable device. --

Please insert immediately following the title "Description of the Preferred Embodiments", appearing at page 10, line 5, and immediately before the paragraph beginning at page 10, line 6, the following three new paragraphs:

-- Herein, throughout the specification of the present invention, including the claims thereof, acronyms are used for referring to several particular types of protocols for using network links, and, associated devices and systems, where the acronyms, and the particular types of protocols, are well known, taught about, and used, in the field and art of the present invention. Additionally, herein, acronyms are used for referring to particular types of electronic messaging services or systems, where the acronyms, and the particular types of electronic messaging, are well known, taught about, and used, in the field and art of the present invention. Additionally, herein, a trademark/trade name and acronyms are used for referring to particular types of networks, where the trademark/trade name, the acronyms, and the particular types of networks, are well known, taught about, and used, in the field and art of the present invention. --

-- The network protocol acronyms appearing in the specification of the present invention, along with the spelled out full name of each acronym, or the spelled out full generic technical name associated with an acronym, consistent with the field and art of the present invention, are as follows:

WAP: wireless application protocol.

GSM: global system mobile telecommunications.

CDMA: code division multiple access.

IS-136: second generation mobile phone system.

PDC: personal digital cellular.

EDGE: enhanced data rates for global system mobile telecommunications evolution.

WCDMA: wideband code division multiple access.

GPRS: general packet radio service.

UMTS: universal mobile telecommunications system.

Iridium: network protocol.

-- The electronic messaging acronyms appearing in the specification of the present invention, along with their spelled out full names, consistent with the field and art of the present invention, are as follows:

SMS: short messaging service.

EMS: enhanced messaging service.

MMS: multimedia messaging system. --

-- The network trademark/trade name and acronyms appearing in the specification of the present invention, along with the spelled out full generic technical name associated with the trademark/trade name, or the spelled out full name of each acronym, consistent with the field and art of the present invention, are as follows:

Bluetooth: wireless personal area network.

LAN: local area network.

WAN: wide area network.

Please replace the paragraph beginning at page 13, line 18, and ending at page 14, line 2, with the following rewritten paragraph:

-- Reference is now made to Fig. 2, which is a simplified diagram showing a GSM device ~~24~~25 such as a mobile telephone. The GSM device comprises a SIM which consists of one or more integrated circuits where at least one of those contains personalized data that supports authentication, encryption and decryption for the secure link 14. The SIM both identifies the mobile telephone and makes it impossible for other devices to impersonate that telephone, thus providing authentication and secure access to a charge account corresponding to the respective mobile telephone user. --

Please replace the paragraph beginning at page 14, line 19, and ending at page 15, line 8, with the following rewritten paragraph:

-- During the log-in process it identifies its secure link, for example by giving an associated mobile telephone number. The identification may be retrieved from storage or

entered manually by the user. The associator 16 receives the identification (e.g. mobile telephone number). It may need to translate the received identification into a different identification appropriate to the communicator 10, and the translation may be carried out by the associator 16 itself or through external translation services, for example by accessing a home location register (HLR). The associator 16 then uses the communicator 10 to contact the mobile telephone in any appropriate way. A timer ~~23~~21 is operated, giving the owner of the mobile telephone a fixed time to reply and confirm the identity of the user. Additionally or alternatively, a failure counter 24 counts unsuccessful attempts to establish the authentication, stopping the authentication operation when a predetermined threshold is reached. --

Please replace the paragraph beginning at page 19, line 18, and ending at page 20, line 23, with the following rewritten paragraph:

-- Reference is now made to Fig. 4 which is a simplified block diagram showing a further embodiment of verification apparatus according to the invention, with component parts shown in greater detail. A non-authenticatable device such as a PDA ~~30~~31 communicates wirelessly via network access points 32, to a LAN/WAN 34, which itself may be wired or wireless. The LAN may be connected directly (or indirectly) to a cellular Internet authentication portal 36, and may be a means of providing the user with access to the Internet or any other data network or services. The portal 36 preferably appears to the PDA ~~30~~31 as a standard Internet authentication device to which it logs in as normal. The login process can be carried out manually or can be automated as desired. The number of the user's mobile telephone may be supplied as the login username or as a separate part of the login procedure. The portal begins to run a timer to timeout the authentication after a predetermined time limit. Optionally the portal may also set up a counter to limit the number of login attempts to reduce the risk of hacking. The portal is connected directly or indirectly to a short message service center SMS-C 38, the network element that manages SMS messaging. The SMS-C 38 sends an SMS message via MSC 40, BSC 42 and cellular base stations 44 to SIM protected mobile telephone 46. The user thus receives a request telling him to press reply in order to activate his network connection. In a further enhancement, the user may be asked to provide a password. The SMS itself is usually encrypted and the SIM supports authentication to make it clear that it is only the intended mobile telephone that is replying. The mobile telephone replies to the SMS. All SMS

messages have an address of origin, which is usually not passed on in Internet-based SMS. In order to enable a reply, the SMS message as sent may be provided with a telephone number of the authenticator to allow a reply to reach the authenticator. The user is then authorized to access the Internet or other data network via the LAN and his use of the LAN may then be charged to his mobile telephone. --

Please replace the paragraph beginning at page 22, line 20, and ending at page 22, line 22, with the following rewritten paragraph:

-- In the preferred embodiment, the authentication method does not require any special hardware or software to be installed on the PDA ~~30~~31. The PDA works with a standard browser and standard network interface units. --

Please replace the paragraph (sentence) beginning at page 23, line 21, and ending at page 23, line 21, with the following rewritten paragraph (sentence):

-- A single network server ~~22~~18 may be used to support many carriers. --